2018 HCCA Compliance Institute
HIPAA Update:
Policy & Enforcement

Policy Update:
Marissa Gordon-Nguyen
HHS OCR Senior Advisor
OCR Responds to Nation’s Opioid Crisis

- Opioid abuse crisis and national health emergencies have heightened concerns about providers’:
  - ability to notify patients’ family and friends when a patient has overdosed
  - reluctance to share health information with patients’ families in an emergency or crisis situation, particularly patients with serious mental illness and substance use disorder
  - uncertainty about HIPAA permissions for sharing information when a patient is incapacitated or presents a threat to self or others

New OCR Guidance on HIPAA and Information Related to Mental and Behavioral Health

- Opioid Overdose Guidance (issued 10/27/2017)
- Updated Guidance on Sharing Information Related to Mental Health (new additions to 2014 guidance)
- 30 Frequently Asked Questions
- New Materials for Professionals and Consumers
  - Fact Sheets for patients, families, and health care providers
  - Information-sharing Decision Charts
Dangerous Patients and Public Safety Disclosures

- Disclosures are permitted without the patient’s authorization or permission to law enforcement, family, friends or others who are in a position to lessen the threatened harm—when disclosure “is necessary to prevent or lessen a serious and imminent threat to the health or safety of the patient or others.”
- Disclosures must be consistent with applicable law.

Where to Find OCR’s New Materials

- For professionals: https://www.hhs.gov/hipaa/for-professionals/index.html > Special Topics > Mental Health & Substance Use Disorders
- For consumers: https://www.hhs.gov/hipaa/for-individuals/index.html > Mental Health & Substance Use Disorders
- Mental Health FAQ Database: https://www.hhs.gov/hipaa/for-professionals/faq/mental-health
- Future FERPA and HIPAA Joint Guidance
### Proposed Changes to HIPAA Privacy and Enforcement Rules

- NPRM on Presumption of Good Faith of Health Care Providers
- NPRM on Changing Requirement to Obtain Acknowledgment of Receipt of Notice of Privacy Practices
- Request for Information on Distribution of a Percentage of Civil Monetary Penalties or Monetary Settlements to Harmed Individuals

### Future HIPAA Guidance

- Texting
- Social Media
- Encryption
Cybersecurity Resources


- Health Information Technology Portal [http://hipaaQsportal.hhs.gov](http://hipaaQsportal.hhs.gov)


Enforcement Update:
Iliana L. Peters
Shareholder, Polsinelli, PC
HIPAA Breach Highlights

September 2009 – December 31, 2017

- Approximately 2,178 reports involving a breach of PHI affecting 500 or more individuals
- Theft and Loss are 46% of large breaches
- Hacking/IT now account for 19% of incidents
- Laptops and other portable storage devices account for 25% of large breaches
- Paper records are 21% of large breaches
- Individuals affected are approximately 176,589,175
- Approximately 307,061 reports of breaches of PHI affecting fewer than 500 individuals

HIPAA Breach Highlights

500+ Breaches by Type of Beach as of December 31, 2017

- Loss: 8%
- Unauthorized Access/Disclosure: 27%
- Other: 4%
- Improper Disposal: 3%
- Unknown: 1%
HIPAA Breach Highlights

500+ Breaches by Location of Beach as of December 31, 2017

- Paper Records: 21%
- Desktop Computer: 10%
- Laptop: 16%
- Portable Electronic Device: 9%
- Network Server: 17%
- Email: 11%
- EMR: 6%
- Other: 10%

General Enforcement Highlights

- Over 171,161 complaints received to date
- Over 25,637 cases resolved with corrective action and/or technical assistance
- Expect to receive 17,000 complaints

As of 12/31/2017
Recent Enforcement Actions

- April 24, 2017: CardioNet
  - $2,500,000
  - $2.5 million settlement shows that not understanding HIPAA requirements creates risk
- May 10, 2017: Memorial Hermann Health System (MHHS)
  - $2,400,000
  - Texas health system settles potential HIPAA violations for disclosing patient information
  - $387,200
  - Careless handling of HIV information jeopardizes patient’s privacy, costs entity $387k
- December 18, 2017: 21st Century Oncology
  - $2,300,000
  - $2.3 Million Levied for Multiple HIPAA Violations at NY-Based Provider
- February 1, 2018: Fresenius Medical Care North America (FMCNA)
  - $3,500,000
  - Five breaches add up to millions in settlement costs for entity that failed to heed HIPAA’s risk analysis and risk management rules
- February 13, 2018: Filefax, Inc.
  - $100,000
  - Consequences for HIPAA violations don’t stop when a business closes

Audit Update:
Marissa Gordon-Nguyen
Audit Program

• Purpose: Identify best practices; uncover risks and vulnerabilities not identified through other enforcement tools; encourage consistent attention to compliance
  • Also hope to learn from this next phase in structuring permanent audit program

Audit Program Purpose & Status

• Support Improved Compliance
• Identify best practices; uncover risks & vulnerabilities; detect areas for technical assistance; encourage consistent attention to compliance
  – Intended to be non-punitive, but OCR can open up compliance review
• Learn from this phase in structuring permanent audit program
• Develop tools and guidance for industry self-evaluation and breach prevention
• Desk audits of covered entities completed – Sept 2017
• Desk audits of business associates completed – Dec 2017
Audited Covered Entities

Audited CEs (166)

- Provider: 89%
- Health Plan: 10%
- Health Care Clearinghouse: 1%

Audited Health Care Providers

Provider Sub-Categories (150)

- Practitioner: 55%
- Pharmacy: 18%
- Hospital: 17%
- Health System: 3%
- Other: 3%
- Skilled Nursing Facility: 2%
- Elder Care: 1%

<table>
<thead>
<tr>
<th>Category</th>
<th>Number of Providers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Practitioner</td>
<td>83</td>
</tr>
<tr>
<td>Pharmacy</td>
<td>27</td>
</tr>
<tr>
<td>Hospital</td>
<td>25</td>
</tr>
<tr>
<td>Health System</td>
<td>5</td>
</tr>
<tr>
<td>Other</td>
<td>5</td>
</tr>
<tr>
<td>Skilled Nursing Facility</td>
<td>3</td>
</tr>
<tr>
<td>Elder Care</td>
<td>2</td>
</tr>
</tbody>
</table>
Covered Entity Desk Audit Controls

Privacy Rule Controls
- Notice of Privacy Practices & Content Requirements
  \([§164.520(a)(1) \& (b)(1)]\)
- Provision of Notice – Electronic Notice
  \([§164.520(c)(3)]\)
- Right to Access
  \([§164.524(a)(1), (b)(1), (b)(2), (c)(2), (c)(3), (c)(4), (d)(1), (d)(3)]\)

Breach Notification Rule Controls
- Notification by a Business Associate
  \([§164.410, with reference to Content of Notification §164.404(c)(1)]\)

Security Rule Controls
- Security Management Process -- Risk Analysis
  \([§164.308(a)(1)(ii)(A)]\)
  \([§164.308(a)(1)(ii)(B)]\)

Audited Business Associates

Audited BAs (41)
Business Associate
Desk Audit Controls

<table>
<thead>
<tr>
<th>Breach Notification Rule Controls</th>
<th>Notification by a Business Associate [§164.410, with reference to Content of Notification §164.404(c)(1)]</th>
</tr>
</thead>
</table>

Ratings

<table>
<thead>
<tr>
<th>Rating</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>The audit results indicate the entity is in compliance with both goals and objectives of the selected standards and implementation specifications.</td>
</tr>
<tr>
<td></td>
<td>The audit results indicate that the entity substantially meets criteria; it maintains appropriate policies and procedures, and documentation and other evidence of implementation meet requirements.</td>
</tr>
<tr>
<td>2</td>
<td>Audit results indicate entity efforts minimally address audited requirements; analysis indicates that entity has made attempts to comply, but implementation is inadequate, or some efforts indicate misunderstanding of requirements.</td>
</tr>
<tr>
<td>3</td>
<td>Audit results indicate the entity made negligible efforts to comply with the audited requirements - e.g. policies and procedures submitted for review are copied directly from an association template; evidence of training is poorly documented and generic.</td>
</tr>
<tr>
<td>4</td>
<td>The entity did not provide OCR with evidence of serious attempt to comply with the Rules and enable individual rights with regard to PHI.</td>
</tr>
</tbody>
</table>
### CE Desk Audit Ratings

<table>
<thead>
<tr>
<th>Element #</th>
<th>Provision</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>P55</td>
<td>Notice</td>
<td>2</td>
<td>34</td>
<td>40</td>
<td>11</td>
<td>16</td>
<td>0</td>
</tr>
<tr>
<td>P58</td>
<td>eNotice</td>
<td>59</td>
<td>16</td>
<td>4</td>
<td>6</td>
<td>15</td>
<td>3</td>
</tr>
<tr>
<td>P65</td>
<td>Access</td>
<td>1</td>
<td>10</td>
<td>27</td>
<td>54</td>
<td>11</td>
<td>0</td>
</tr>
<tr>
<td>BNR 12</td>
<td>Timeliness</td>
<td>67</td>
<td>6</td>
<td>2</td>
<td>9</td>
<td>12</td>
<td>7</td>
</tr>
<tr>
<td>BNR13</td>
<td>Content</td>
<td>14</td>
<td>15</td>
<td>24</td>
<td>38</td>
<td>7</td>
<td>5</td>
</tr>
<tr>
<td>S2</td>
<td>Risk Analysis</td>
<td>0</td>
<td>9</td>
<td>20</td>
<td>21</td>
<td>13</td>
<td>0</td>
</tr>
<tr>
<td>S3</td>
<td>Risk Management</td>
<td>2</td>
<td>2</td>
<td>15</td>
<td>28</td>
<td>16</td>
<td>0</td>
</tr>
</tbody>
</table>

### BA Desk Audit Ratings

<table>
<thead>
<tr>
<th>Element #</th>
<th>Provision</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>BNR17</td>
<td>Notice to CEs</td>
<td>0</td>
<td>2</td>
<td>4</td>
<td>3</td>
<td>0</td>
<td>32</td>
</tr>
<tr>
<td>S2</td>
<td>Risk Analysis</td>
<td>3</td>
<td>4</td>
<td>16</td>
<td>12</td>
<td>6</td>
<td>0</td>
</tr>
<tr>
<td>S3</td>
<td>Risk Management</td>
<td>0</td>
<td>5</td>
<td>8</td>
<td>21</td>
<td>7</td>
<td>0</td>
</tr>
</tbody>
</table>
Industry Take-Away

Best Outcomes
- Providing timely notice of breach
- Posting of NPP on website
- Providing required NPP content

Most Room for Improvement
- Risk Management
- Risk Analysis
- Enabling Individual Access

OCR will examine entity practices for lessons learned that can be shared in technical assistance

OCR is working to enhance technical assistance in those areas

Top Ten Compliance Issues:
Iliana L. Peters
Recurring Compliance Issues

- Pattern of Disclosure of Sensitive Paper PHI
- Business Associate Agreements
- Risk Analysis
- Failure to Manage Identified Risk, e.g. Encrypt
- Lack of Transmission Security
- Lack of Appropriate Auditing
- No Patching of Software
- Insider Threat
- Improper Disposal
- Insufficient Data Backup and Contingency Planning

Recent FTC Enforcement Actions

- Feb 27, 2018:
  - PayPal Settles FTC Charges that Venmo Failed to Disclose Information to Consumers About the Ability to Transfer Funds and Privacy Settings; Violated Gramm-Leach-Bliley Act
- Nov 29, 2017:
  - FTC Gives Final Approval to Settlements with Companies that Falsely Claimed Participation in Privacy Shield
- Nov 8, 2017:
  - FTC Gives Final Approval to Settlement with Online Tax Preparation Service
- Aug 15, 2017:
  - Uber Settles FTC Allegations that It Made Deceptive Privacy and Data Security Claims
OCR Resources

- https://www.hhs.gov/hipaa/for-professionals/privacy/index.html

Polsinelli Resources

- Polsinelli serves clients nationally:
  - https://www.polsinelli.com/
  - 100+ services and 70+ industry areas
  - 800+ Attorneys
  - https://www.polsinelli.com/professionals/ipeters

- 20 Cities – Metropolitan offices in:
  - Atlanta
  - Boston
  - Chicago
  - Dallas
  - Denver
  - Houston
  - Kansas City
  - Los Angeles
  - Nashville
  - New York
  - Phoenix
  - St. Louis
  - San Francisco
  - Silicon Valley
  - Washington, D.C.
  - Wilmington